UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,647	02/22/2002	Eiichi Horita	10746/31	8170

26646 7590 10/18/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/080,647	HORITA ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5 IDS's*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined.

2. Based upon Applicant's specification (see Specification, p. 16, lines 8-10), it is being presumed that each of the "digital signature generation parts" as recited in the claims refer to separate devices that are communicatively connected.

Priority

3. The instant application claims priority to Japan Patent Application No. 2001-047338, filed 22 February 2001.

Information Disclosure Statement

4. The following Information Disclosure Statements in the instant application have been fully considered, except as otherwise noted:

IDS filed 2 April 2002.

IDS filed 26 March 2004.

IDS filed 13 May 2004.

IDS filed 11 August 2004.

IDS filed 14 June 2005.

5. The two foreign patent documents cited in the IDS filed 2 April 2002 are not in English and have not been considered.

6. The second and third documents cited in the IDS filed on 26 March 2004 are referenced by their Japanese patent application numbers, rather than their publication numbers. The publication numbers are 10-198272 and 2001-142398, respectively, and the IDS has been corrected.

Drawings

7. The drawings are objected to because in item 15 in the drawings, the word "SINGED" should be "SIGNED."

8. The drawings are objected to because the reference to figure 6 on page 27, line 8 of the specification should refer instead to figure 7.

9. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: items 2, 15, 16, 17, 18, 19, and step 64.

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: item "1" on page 16, line 35.

11. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

12. The incorporation of essential material in the specification by reference to an unpublished U.S. application, foreign application or patent, or to a publication is improper. Applicant is required to amend the disclosure to include the material incorporated by reference, if the material is relied upon to overcome any objection, rejection, or other requirement imposed by the Office. The amendment must be

accompanied by a statement executed by the applicant, or a practitioner representing the applicant, stating that the material being inserted is the material previously incorporated by reference and that the amendment contains no new matter. 37 CFR 1.57(f).

The specification describes the generation of partial digital signatures in the absence of a trusted third party simply by referencing a publication by Boneh et al. (see Specification, page 20, lines 8-14). This material is essential to the claimed invention and must be explicitly described in the disclosure.

Claim Objections

13. Claims 7, 10, and 15-20 are objected to because of the following informalities: They lack transitional phrases. For purposes of the prior art, it is being presumed that each limitation is being recited in an open-ended manner, beginning after the first instance of the word "wherein." Appropriate correction is required.

14. Claim 5 is objected to because of the following informalities: It is dependent upon itself. It is being presumed that claim 5 is dependent upon claim 4. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claims 2, 5, 8, and 11 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: It is not shown how the transformation number is used in the transformation process.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

16. Claim 1, 3, 7, 9, 13, 15, 17, and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000.

As per claims 1, 7, 13, 15, 17, and 19, Malkin discloses a system wherein a set of servers select a partial signature key based upon the client's specification, thereby obviating the need for a trusted third party. Each uses a hash derived from the partial signature key to sign a message (i.e. a document), and sends back the computed

partial signature (see Sections 3.1 and 4). The signatures are combined when a t-ou-0of-k threshold is reached, producing a combined signature (see Section 3.1.1).

As per claims 3 and 9, a mechanism is disclosed to identify corrupted signatures sent by servers (see section 4.1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 4, 6, 10, 12, 14, 16, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000 as applied to claim 1 et al. above, and further in view of U.S. Patent No. 5,610,982 to Micali.

Malkin only discloses the passing of the computed partial signature by the server, not suggesting to also pass the document.

Micali discloses the passing of the document with a certificate having the signature, and suggests that this keeps the members accountable for the certificates they cause to issue (see column 9, lines 40-63).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Malkin by passing the document with the signature, as disclosed by Micali, as this keeps the members accountable for the certificates they cause to issue.

18. Claims 2 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000 as applied to claim 1 et al. above, and further in view of U.S. Patent No. 4,405,829 to Rivest et al.

Malkin does not disclose a signature key generating algorithm using an LCM function.

Rivest discloses a signature key generating algorithm (RSA) that uses the LCM function in generating a key from the arguments (see column 5, lines 9-12), and suggests that this algorithm allows for the usage of public keys in signature generation (see column 3, lines 64-68).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Malkin by using the algorithm of Rivest for signature generation, as this allows for the usage of public keys in signature generation.

19. Claims 5 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information

Survivability Conference and Exposition, 2000 in view of U.S. Patent No. 5,610,982 to Micali as applied to claim 4 et al. above, and further in view of U.S. Patent No. 4,405,829 to Rivest et al.

Malkin and Micali do not disclose a signature key generating algorithm using an LCM function.

Rivest discloses a signature key generating algorithm (RSA) that uses the LCM function in generating a key from the arguments (see column 5, lines 9-12), and suggests that this algorithm allows for the usage of public keys in signature generation (see column 3, lines 64-68).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Malkin and Micali by using the algorithm of Rivest for signature generation, as this allows for the usage of public keys in signature generation.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,097,504 to Camion et al. discloses a cooperative signature generation scheme.

U.S. Patent No. 5,638,447 to Micali discloses a technique for generating verifiable multi-party signatures.

U.S. Patent No. 5,708,714 to Lopez et al. discloses a system for cooperative signature generation.

U.S. Patent No. 5,825,880 to Sudia et al. discloses multi-party signature generation using a seed froma third party.

U.S. Patent No. 5,960,086 to Atalla discloses the use of end-to-end session signatures.

U.S. Patent No. 6,088,798 to Shimbo discloses a multi-party signature generation system using elliptic curves.

U.S. Patent Application Publication No. 2002/0076052 to Yung et al. discloses partial signature generation using a shared random number generating algorithm.

U.S. Patent Application Publication No. 2003/0120931 to Hopkins et al. discloses a technique for generating group signatures using primes.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

October 13, 2005